DEPARTMENT OF WORKFORCE DEVELOPMENT
DIVISION OF ECONOMIC SUPPORT and
DIVISION OF UNEMPLOYMENT INSURANCE
ADMINISTRATOR'S MEMO SERIES

NOTICE 00-12

ISSUE DATE: 08/07/2000

DISPOSAL DATE: Ongoing

RE: SAFEGUARDING FEDERAL TAX INFORMATION

To: County Department of Human Services Directors
County Department of Social Services Directors
County Economic Support Managers/Supervisors/Lead Workers
Tribal Chairpersons/Human Services/Economic Support Directors
Area Administrators/Assistant Area Administrators

From: Jennifer L. Noyes
DES Administrator

Bruce Hagen
DUI Administrator

Introduction

This Administrator's Memo replaces DES Administrator's Memo 92-22, issued March 17, 1992, and all subsequent safeguard related communications by DES and DUI. It includes all recent federal changes to the IRS safeguard requirements and the IRS state agency safeguard review recommendations.

The Department of Workforce Development (DWD), Division of Unemployment Insurance (DUI), Public Assistance Fraud Section (PAFS), has responsibility for administration of the safeguarding of federal tax data used in Wisconsin for the income maintenance and economic support programs. The attached Safeguard Policy provides state and local agencies with the current Internal Revenue Service (IRS) Tax Information Security Guidelines for protecting federal tax return information.

Authorization

Federal Public Law 98-369, the Deficit Reduction Act of 1984 (DEFRA), requires as part of the mandatory Income and Eligibility Verification System (IEVS) that states conduct computer matches of their income maintenance caseloads against the tax information available from the Social Security Administration's BENDEX Wage file of earnings and against the IRS file of

unearned income. The data from these two computer matches are subject to the IRS safeguard requirements. The information received from the IRS for the Treasury Offset Program (TOP), formerly known as the Federal Tax Refund Offset Program (FTROP), is also subject to the IRS safeguard requirements.

Purpose

The purpose of the Safeguard Policy is to ensure state and local agency compliance with the Internal Revenue Service (IRS) Tax Information Security Guidelines for protecting federal tax return information. It contains the most current IRS safeguard requirements and state/federal recommendations for meeting those requirements. Included is an updated annual training packet and staff authorization sheet, discussion of safeguard verification issues, and an agency self-review checklist.

Monitoring

Safeguard rules require regular monitoring of agencies accessing federal tax data. DUI conducts this monitoring through (1) Receipt of the annual staff authorization sheets. (2) Receipt of an annual agency self-review checklist, and (3) Regular DUI safeguard reviews of local agencies.

SAFEGUARD POLICY
IEVS and FTROP/TOP

BACKGROUND

Federal Public Law 98-369, the Deficit Reduction Act of 1984 (DEFRA), requires as a part of the mandatory Income and Eligibility Verification System (IEVS) requirement that states do computer matching of their income maintenance caseloads against two sources of federal tax information. These sources are the Social Security Administration's BENDEX wage file of earnings from self-employment and wages, and the Internal Revenue Service (IRS) file of unearned income. The tax information from these two computer matches is subject to the safeguard standards issued in IRS Publication 1075, Tax Information Security Guidelines. The IRS safeguard guide provides standards of compliance in seven areas:

The Federal Tax Refund Offset (intercept) Program (FTROP), now known as the Treasury Offset Program (TOP), to recover delinquent benefit overpayments in closed cases was implemented in 1993. The TOP program requires an exchange of information with the IRS. The information received from the IRS for the TOP program is subject to the same IRS safeguard requirements described for the IEVS program. TOP documents containing IRS tax information must be treated as safeguarded documents.

STATE AGENCY SAFEGUARD RESPONSIBILITY

The state agency responsible for the safeguard program associated with IEVS and TOP federal tax information, is the Division of Unemployment Insurance (DUI), Bureau of Program Integrity (BPI), Public Assistance Fraud Section (PAFS). The DUI Safeguard Manager is responsible for directing the operation of the safeguard program for IEVS and TOP IRS federal tax return information in Wisconsin.

The DUI Safeguard Manager will maintain a statewide database to include compliance with the annual safeguard training requirement of staff, the tracking and destruction of safeguarded documents, and staff authorized for access to safeguarded information. The DUI Safeguard Manager will ensure state compliance with the IRS safeguard requirements, including: the regular reviews of local agencies, annual reports to the IRS, annual training of authorized staff, review and approval of local agency requests for staff access to federal tax data, as well as policy development and communications with local agencies.

The DUI Safeguard Manager will coordinate regular agency safeguard reviews of all local agencies authorized to receive IRS tax information. S/he will also coordinate and assist in the IRS State Safeguard Reviews of local agencies.

LOCAL AGENCY SAFEGUARD RESPONSIBILITIES

All local agencies receiving IRS tax information from the IEVS and TOP sources are responsible for the implementation and enforcement of the IRS safeguard policy described in this document. Each agency must have an individual designated as their “Safeguard Custodian" responsible for administering the safeguard requirements. The agency director will be designated the Safeguard Custodian unless the agency specifies someone else. The DUI Safeguard Manager should be notified whenever there is a change in an agency’s Safeguard Custodian.

SAFEGUARD CUSTODIAN RESPONSIBILITIES:

The local agency Safeguard Custodian is the primary contact person for the safeguard program for state and federal safeguard officials. The local agency Safeguard Custodian is responsible for requesting from DUI access authorization for agency staff, removal of authorization for staff, ensuring that all authorized staff complete the annual safeguard training and authorization requirement, conducting an annual local safeguard self-assessment, and coordinating state and federal local agency safeguard program reviews. The Safeguard Custodian is also responsible for the receipt of the safeguarded documents when paper documents are used, disposition of those documents, and tracking of the documents through the use of safeguard logs. In addition, the Safeguard Custodian is responsible for the safeguarding and tracking of CARES screen prints containing tax information, destruction of completed safeguarded information, both IEVS and TOP, and safeguard reporting to the DUI, Bureau of Program Integrity, Public Assistance Fraud Section, formerly the Office of Inspector General (OIG).

SAFEGUARD RESPONSIBILITIES:

1. SAFEGUARD ACCESS

    1.1. Each agency Safeguard Custodian shall maintain a listing of all authorized persons in the agency at a location accessible by agency staff. The authorization listing must be updated annually as well as whenever a change in agency staff needing access to the tax information (including deletions) occurs. A copy will be submitted to the Safeguard Manager in DUI who will review the listing and may question or deny authorization to persons without a justifiable

need to access the tax information. The authorization listing should include the following information:

i. Names of authorized staff members;
ii. Job function of staff members (i.e. Economic Support Specialist [ES]);
iii. Justification for access, unless self-evident (i.e., case management or supervisory responsibility).

1.2. Each agency staff member authorized to access federal tax information must annually complete and sign an Authorization Sheet attesting that s/he has completed the annual safeguard training and understands the safeguard policies and penalties. The signed Authorization Sheets are to be submitted to the Safeguard Manager in DUI.

2. SAFEGUARD AWARENESS

2.1. Agency staff, including the agency's Safeguard Custodian and management, should be aware of the following safeguard principles:

i. Access to federal tax information must always be on a "need-to-know" basis.
ii. Disclosure of federal tax information is permitted only to authorized persons and only for the purpose of eligibility verification.
iii. Federal tax information, whether paper documents or on-line data, must be secured at all times and not commingled with other documents or files.
iv. Access to federal tax information must be reported and tracked. When paper documents are involved, a safeguard log must be used.
v. Federal tax information must be destroyed upon completion of use.
vi. Unauthorized disclosure or inspection of federal tax information is a federal crime.

2.2. Agency staff, including the agency's Safeguard Custodian and management, need to be aware of the two types of unauthorized activity involving federal tax information:

i. Unauthorized disclosure.
ii. Unauthorized inspection.

2.3. Agency staff, including the agency's Safeguard Custodian and management, need to be aware of the two types of penalties that are possible consequences of the unauthorized activity with federal tax information:

i. Criminal.
ii. Civil.

2.4. Agency staff, including the agency's Safeguard Custodian and management, need to know how to identify safeguard-authorized staff in the agency by access to the current safeguard authorized staff listing.

2.5. Agency staff, including the agency's Safeguard Custodian and management, need to know where to access the state's safeguard policy either in the agency's files or on the DUI Internet home page.

3. SAFEGUARD TRAINING

A training packet (Attachment I), consisting of a summary description of the safeguard requirements, penalties for intentional unauthorized disclosure and an authorization sheet that all authorized staff must sign annually is attached. The IRS training packet is to be delivered annually to all authorized staff and prior to initial access for all new staff. The signed authorization sheets are to be sent to the DUI Safeguard Manager annually. Agency staff need to retain a copy of the safeguard training packet at their workstations.

DUI will annually update the Safeguard Training Packet and send it to all affected agencies. The annual update notice will include the due date for submission of the annual list of authorized staff and individual authorization sheets to DUI.

Updated safeguard information is to be sent to the DUI Safeguard Manager promptly. We recommend that information be sent immediately when only a single change is involved, and not be held more than a week when collecting multiple changes.

4. SAFEGUARD RECORD KEEPING

Safeguarded match reports and CARES screen prints of federal tax data need to be accompanied by a "Safeguard Tracking/Disposition Log" (Attachment III) for each separate document. These logs are used to record all activities occurring to their specific documents. The activities to be recorded include the receipt or creation of the document by the agency, distribution to staff, access by staff, and eventual destruction. Completed logs are to be returned to the DUI Safeguard Manager.

Any safeguarded document in an agency's possession must have a safeguard log to comply with the safeguard record-keeping requirement. If a safeguard log does not accompany the safeguarded document, the agency needs to create a log. See Attachment IV for a model safeguard log to use for this purpose.

5. PHYSICAL SECURITY

Physical security for safeguarded documents is based on a layered security design in the custodial agency. Agencies have discretion in the design of their safeguard system to conform to the existing physical structure of the building where the agency is located. The security design needs to prevent unauthorized individuals from being able to access the agencies safeguarded documents and information. The desired design will have three layers of physical security: office, area/room, and container.

5.1. Office Security

The most desirable restriction is the use of physical barriers such as locked doors. Access to the work areas of the agency where federal tax information is used or stored should be restricted to persons having legitimate business with the agency. Visitors should be escorted while in secured areas of the office.

5.2 Storage Area Security

The agency must establish an on-site location for the storage of safeguarded documents that are not in use by agency staff, or are awaiting destruction. This storage area should have most of the following features:

i. An interior, windowless room, or located above the ground floor.
ii. An exterior, windowed, ground floor storage area must have the window secured from possible breakage and entry.
iii. Entry to the room must be restricted by a physical barrier, i.e., a locked door, to prevent unauthorized staff from accessing the storage area.
iv. The storage area must be secured/locked when not occupied by authorized staff.
v. Security should be automatic, i.e., a door that will close and lock automatically.
vi. After work hours, access to the storage area must be controlled and limited to persons having a legitimate work related reason to be in the area.

5.3. Container Security

The agency must store safeguarded documents in a container that should have most of the following features:

i. lockable with welded metal construction.
ii. Containers having only a business office quality integrated key lock should have a lock bar added to the container.
iii. The container should be locked when authorized staff are not in the storage area.
iv. Keys/combinations to the container should be limited as much as possible.

5.4. Staff Storage Security

i. Safeguarded documents in temporary staff custody must be secured when not in use in a locked, welded metal container.
ii. The staff storage container should be locked when authorized staff are not in their work area.
iii. Local agency safeguard policy should minimize safeguarded document storage by staff.

5.5. Agency Safeguarding

i. Only authorized staff should open mail containing safeguarded documents.
ii. Safeguarded documents should be transported within a building in a sealed package, and hand-carried by safeguard authorized staff.
iii. Safeguarded documents being sent to another geographic site must be secured in a sealed package, labeled either “Confidential” or “Safeguarded”, and addressed to a safeguard authorized individual.
iv. The agency should have a control system in place for the use of locks, keys, and combinations used for safeguarding documents, including a policy to prevent the compromising of combinations when staff leave.
v. The agency should have an accountability record system for keys, including a policy prohibiting unauthorized duplication of keys, and a periodic inventory of keys.

vi. The agency must report all intentional unauthorized violations of the safeguard policy to the DUI Safeguard Manager.
vii. The agency should have a policy and staff must be aware that federal tax information can only be used or disclosed for the purpose of verification of eligibility.

6. ON-LINE/DATA SAFEGUARDING

Federal tax information located in the CARES system is secured, tracked, monitored, and destroyed by the CARES security system. Local agencies need to ensure that staff are aware of the strict limitations on the disclosure of this safeguarded information. The agency's policy on the creation and handling of safeguarded documents from the CARES screens must fully safeguard the data. DUI recommends that local agencies adopt the following or similar policies:

i. Prohibit staff creation of safeguarded documents by screen printing CARES tax match screens or writing down federal tax information. The exception is the creation of original verification notices.
ii. Prior notification to the agency's Safeguard Custodian when a safeguarded document is created to ensure proper safeguard handling.
iii. Back-up for absent staff with a safeguarded workload be assigned to supervisory staff.

7. DESTRUCTION OF TAX DOCUMENTS/INFORMATION

Upon completion of use, all safeguarded documents from the computer matches, printed CARES screens, and TOP program are to be destroyed. Shredding, to strips of 5/16 inch or less, or burning are recommended. Shredded documents must be cut perpendicular to the printing. Burned documents must be stirred to separate any bundles. The destruction of safeguarded documents should be performed by or supervised by safeguard authorized staff. The destruction of IEVS paper documents must be recorded on the appropriate Safeguard Log prior to its being returned to the DUI Safeguard Manager.

8. ANNUAL AGENCY SAFEGUARD SELF-REVIEW

Local agencies handling federal tax information should conduct an annual internal inspection of their safeguard program. The safeguard self-review needs to focus on staff awareness of safeguarding and when to apply safeguard practices. The conducting of these safeguard self-reviews will help ensure that agency staff remain aware of the safeguard requirements during a time of limited safeguard activity thereby limiting the liability that the agency and staff may be subject to. To assist in doing these self reviews, a Safeguard Self-Review Checklist (Attachment IV) is attached for local agency use.

DUI will send each affected agency a notice of the annual safeguard self-review concurrent with the annual safeguard training notice. The annual safeguard self-review should be conducted prior to the annual safeguard training. The safeguard self-review findings are to be sent to the DUI Safeguard Manager as described in the annual notice.

COMMENTS:

The IEVS matches, including the two federal tax data matches, are now presented as on-line files rather than paper documents. This eliminates the need for safeguarding the paper match reports, filling-out the disposition logs, destroying the safeguarded match documents, and returning the safeguard logs to the PAFS. Please be sure that all agency staff are aware that all print-outs from the two federal tax data matches' are safeguarded documents and must be treated as such. The creation and handling of verification documents by local agencies has been identified as an important safeguard issue. See Attachment II for a discussion of safeguarding verification documents.

TOP continues to have safeguarded paper documents containing IRS tax information. These documents require proper safeguard handling. The IRS tax information, in whatever form, continues to be safeguarded and subject to all the safeguard requirements for disclosure and handling.

With the implementation of the Wisconsin Works program and the use of Job Centers around the state, local agencies having possession of safeguarded documents are often sharing buildings and even work spaces with other local agencies and private contractors. As these agencies and private contractors are not authorized to access the IRS tax information given to local public assistance agencies, their physical proximity creates a potential safeguard disclosure issue. Local public assistance agencies located in a Job Center or other shared work space need to review their practices for handling of on-line safeguarded data and paper safeguarded documents, to ensure that they do not allow inadvertent disclosures in the shared environment.

CENTRAL OFFICE CONTACT: Charles Billings, DUI/PAF Safeguard Manager
(608) 266-9246 Fax (608) 266-7054, or E-mail:
billich@dwd.state.wi.us.

Attachments		Forms
ATTACHMENT I	Federal Tax Information Training Packet	
Part A	Requirements	
Part B	Penalties	
Part C	Authorization Sheet	[UCF-12287 (R. 5/2000]
ATTACHMENT II	Verification of IEVS Safeguarded information	
ATTACHMENT III	Safeguard Tracking Disposition Log	[UCF-12283 (R. 5/2000)]
ATTACHMENT IV	Agency Safeguard Self Review Checklist	[UCF-12284 (R. 5/2000)]

cc: County Board Chairpersons